WE CLAIM:

1. A computer program product operable for controlling a computer to identify a computer file as potentially containing malware, said computer program product comprising:

searching code operable to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;

context identifying code operable to identify a context within said computer file of said one or more target words; and

file identifying code operable if said context matches one or a predetermined set of contexts to identify said computer file as potentially containing malware.

2. A computer program product as claimed in claim 1, wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

words that are indicative of being part of a message embedded within said computer file by a malware author;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author.

3. A computer program product as claimed in claim 1, wherein said predetermined sets of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage;

within executable code; and

within a predetermined proximity to another target word.

4. A computer program product as claimed in claim 1, wherein, if said computer file is identified as potentially containing malware, then malware found code triggers one or more malware found actions.

5. A computer program product as claimed in claim 4, wherein said malware found actions include one or more of:

quarantining said computer file;

deleting said computer file;

issuing a warning message concerning said computer file; and

deleting a portion of said computer file suspect of containing malware.

6. A computer program product as claimed in claim 1, wherein, if said computer file is identified as potentially containing malware, then trigger thresholds associated with one or more other malware identifying processes applied to said computer file are adjusted to be more sensitive.

7. A computer program product as claimed in claim 1, wherein if said computer file is identified as potentially containing malware, then a trigger threshold associated with a heuristic malware identifying process applied to said computer file is set to a more sensitive level.

8. A computer program product as claimed in claim 1, wherein all of said computer file is searched for said target words.

9. A computer program product as claimed in claim 1, wherein only those portions of said computer file matching said predetermined set of contexts are searched for said target words.

10. A computer program product as claimed in claim 1, wherein said malware comprises one or more of a computer virus, a worm and a Trojan.

11. A method of identifying a computer file as potentially containing malware, said method comprising the step of:

searching within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;

identifying a context within said computer file of said one or more target words; and

if said context matches one or a predetermined set of contexts, then identifying said computer file as potentially containing malware.

12. A method as claimed in claim 11, wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

words that are indicative of being part of a message embedded within said computer file by a malware author;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author.

13. A method as claimed in claim 11, wherein said predetermined sets of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage;

within executable code; and

within a predetermined proximity to another target word.

14. A method as claimed in claim 11, wherein, if said computer file is identified as potentially containing malware, then one or more malware found actions are triggered.

15. A method as claimed in claim 14, wherein said malware found actions include one or more of:

quarantining said computer file;

deleting said computer file;

issuing a warning message concerning said computer file; and

deleting a portion of said computer file suspect of containing malware.

16. A method as claimed in claim 11, wherein, if said computer file is identified as potentially containing malware, then trigger thresholds associated with one or more other malware identifying processes applied to said computer file are adjusted to be more sensitive.

17. A method as claimed in claim 11, wherein if said computer file is identified as potentially containing malware, then a trigger threshold associated with a heuristic malware identifying process applied to said computer file is set to a more sensitive level.

18. A method as claimed in claim 11, wherein all of said computer file is searched for said target words.

19. A method as claimed in claim 11, wherein only those portions of said computer file matching said predetermined set of contexts are searched for said target words.

20. A method as claimed in claim 11, wherein said malware comprises one or more of a computer virus, a worm and a Trojan.

21. Apparatus for identifying a computer file as potentially containing malware, said apparatus comprising:

searching logic operable to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library;

context identifying logic operable to identify a context within said computer file of said one or more target words; and

file identifying logic operable if said context matches one or a predetermined set of contexts to identify said computer file as potentially containing malware.

22. Apparatus as claimed in claim 21, wherein said predetermined word library includes one or more of:

words that are names associated with known malware authors;

words that are indicative of being part of a message embedded within said computer file by a malware author;

word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author.

23. Apparatus as claimed in claim 21, wherein said predetermined sets of contexts includes one or more of:

within a script portion of a webpage;

within a comment of a webpage;

within executable code; and

within a predetermined proximity to another target word.

24. Apparatus as claimed in claim 21, wherein, if said computer file is identified as potentially containing malware, then malware found logic triggers one or more malware found actions.

5. Apparatus as claimed in claim 24, wherein said malware found actions include one or more of:

quarantining said computer file;

deleting said computer file;

issuing a warning message concerning said computer file; and

deleting a portion of said computer file suspect of containing malware.

26. Apparatus as claimed in claim 21, wherein, if said computer file is identified as potentially containing malware, then trigger thresholds associated with one or more other malware identifying processes applied to said computer file are adjusted to be more sensitive.

27. Apparatus as claimed in claim 21, wherein if said computer file is identified as potentially containing malware, then a trigger threshold associated with a heuristic malware identifying process applied to said computer file is set to a more sensitive level.

28. Apparatus as claimed in claim 21, wherein all of said computer file is searched for said target words.

29. Apparatus as claimed in claim 21, wherein only those portions of said computer file matching said predetermined set of contexts are searched for said target words.

30. Apparatus as claimed in claim 21, wherein said malware comprises one or more of a computer virus, a worm and a Trojan.